

DIALOG(R)File 351:DERWENT WPI
(c)1996 Derwent Info Ltd. All rts. reserv.

010646794 WPI Acc No: 96-143748/15

XRPX Acc No: N96-120522 *Image available*

Document secrecy management method - encoding of image data when image data of secrecy management embedded on document image re-appears and then carries out decoding

Patent Assignee: (RICO) RICOH KK

Number of Patents: 001

Number of Countries: 001

Patent Family:

CC Number	Kind	Date	Week	
JP 8030759	A	960202	9615	(Basic)

Priority Data (CC No Date): JP 94167921 (940720)

Abstract (Basic): JP 08030759 A

The management method involves forming an image (110) for secrecy management. The image is then converted to Fourier equivalent data (112) and an image data (113) is obtained.

The image data for secrecy management is embedded on a document image (114). When the embedded image (115) reappears, an encoding data is extracted and carries out decoding from the image of documents.

ADVANTAGE - Automates reappearing processing. Eases reading of documents. Prevents alteration of information.

Dwg.3/12

File Segment: EPI

Derwent Class: T01;

Int Pat Class: G06T-001/00

Manual Codes (EPI/S-X): T01-D01; T01-J04B1; T01-J10C

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平8-30759

(43)公開日 平成8年(1996)2月2日

(51)Int.Cl.⁶
G 0 6 T 1/00

識別記号
9365-5H

庁内整理番号
G 0 6 F 15/ 62

F I

技術表示箇所
P

審査請求 未請求 請求項の数5 O L (全 9 頁)

(21)出願番号 特願平6-167921

(22)出願日 平成6年(1994)7月20日

(71)出願人 000006747

株式会社リコー

東京都大田区中馬込1丁目3番6号

(72)発明者 阿部 健

東京都大田区中馬込1丁目3番6号 株式会社リコー内

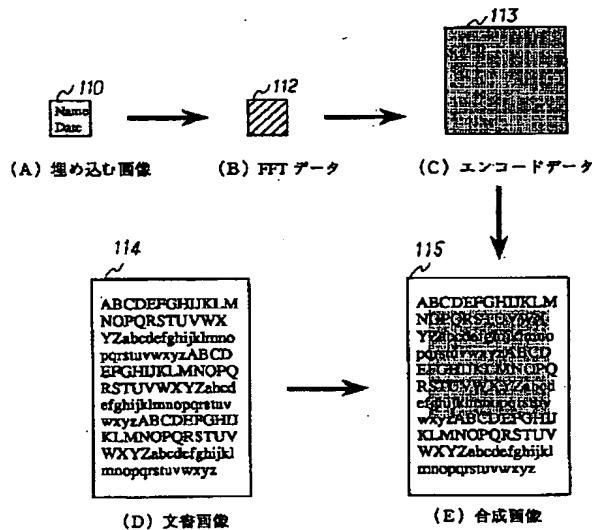
(74)代理人 弁理士 鈴木 誠 (外1名)

(54)【発明の名称】 書類機密管理方法及び画像処理装置

(57)【要約】

【構成】 機密管理用画像110のFFTデータ112を点の集合の形にエンコードしたデータ113を書類画像114と合成することによって、機密管理用画像情報を書類に埋め込む。埋め込んだ機密管理用画像の再現する場合は、書類の画像よりエンコードデータを抽出してデコードし、逆FFTを行なう。

【効果】 書類の複写を繰り返しても機密管理用画像情報を再現可能である。機密管理用画像情報の内容を秘匿でき、その再現処理を自動化できる。



1

【特許請求の範囲】

【請求項1】 機密管理用画像のフーリエ変換データを点の集合の形にエンコードして書類の画像に埋め込むことを特徴とする書類機密管理方法。

【請求項2】 機密管理用画像のフーリエ変換データを点の集合の形にエンコードして書類の画像に埋め込んでおき、該書類またはその複写の画像より、そこに埋め込まれたフーリエ変換データを復元して逆フーリエ変換を行なうことにより該機密管理用画像を再現することを特徴とする書類機密管理方法。

【請求項3】 書類の画像及び機密管理用画像を入力するための手段と、該機密管理用画像のフーリエ変換データを得るための手段と、該フーリエ変換データを点の集合の形にエンコードするための手段と、該エンコード後のフーリエ変換データと該書類の画像とを合成して出力するための手段とを有することを特徴とする画像処理装置。

【請求項4】 書類の画像を読み取って入力するための手段と、該書類の画像より、フーリエ変換データの点の集合の形にエンコードされたデータを抽出するための手段と、該エンコードされたデータをデコードするための手段と、該デコードされたデータの逆フーリエ変換を行ない画像を復元するための手段とを有することを特徴とする画像処理装置。

【請求項5】 復元された画像が予め決められた機密管理用画像であるか判定するための手段とを有することを特徴とする請求項4記載の画像処理装置。

【発明の詳細な説明】

【0001】

【産業上の利用分野】 本発明は、機密書類（文書、図表等）の管理に係わる技術に関する。本発明は特に、流出した機密書類より、その流出経路の追跡等に役立つ情報を当該文書より取得できるようにするための技術に関する。

【0002】

【従来の技術】 企業や官公署等で扱う書類の中には、特定の人、部署、機関等以外には機密を保持したいものが少なくない。このような書類の機密保持のためには、書類の持ち出しや閲覧を制限するとともに書類の複写を制限あるいは管理することが大切である。そのため次のような対策が実施され、あるいは検討されている。

【0003】 (1) 機密書類に「マル秘」マークを表示して取扱者に注意を促す。

(2) 書類を閲覧できる場所を制限し、持ち出しを許さない。

(3) 複写機にパスワードを入力しないと複写できないようにする。

(4) 文書の隅等にバーコード等を付加しておき、複写時にそれを読み込んで複写の履歴として記録保存し、また、複写に新たなバーコードを書き込む。

10

2

しかし、このような対策を講じても、故意に、あるいは不注意から、機密文書そのもの、あるいは、その複写が第三者に渡ってしまう危険性があるため、書類あるいはその複写が外部に流出した場合に、その書類あるいは複写より、その流出元の名称等の流出経路の追跡に役立つ情報を取得できるようにすることも重要である。

【0004】 この流出経路の追跡に係わる従来技術として、特開平4-31075号公報に述べられている「機密文書管理方式」が知られている。これは、情報処理装置によって文書をプリントアウトする際に、文書の配布先毎に異なった場所の1文字だけフォントを変えて出力し、また、このようにしてプリントアウトされた文書の配布先を知りたい場合には、情報処理装置のディスプレイ上で文書中のフォントの変わっている文字の場所を指示することによって、配布先がディスプレイに表示されるというものである。

【0005】

【発明が解決しようとする課題】 しかし、上記「機密文書管理方式」は、次のような難点があるため、その実用性に疑問がある。

【0006】 (1) 文書の複写によりフォントが不明瞭になりやすいため、複写を繰り返した文書、あるいは故意に文字のつぶれ等を生じさせるような条件で複写をした文書からは、その配布先（流出元）を確認することが困難になる。

(2) 上記公報に、フォントが変えられている文字を人が認識して、その位置をポインティング手段によって指示する実施例が提示されていることからも理解されるように、配布先を示すためフォントが変えられた文字の検出を自動的に行なうことは容易でなく、特に、複写を繰り返した文書ではより困難であるため、文書の配布先（流出元）認識の自動化が難しい。

(3) 文書の出力に使用できるフォントが制限され、あるいは、配布先を明示するために独自のフォントを用意する必要が生じる。

(4) 上記公報の記載によれば、機密文書であることを明示せずに管理できるということであるが、特定位置の文字のフォントを変える方法であるから明示的であることは明らかであり、しかも比較的容易に改竄することができる。

(5) 文書を最初に出力する際に特定の場所の1文字のフォントを変化させるという方法であり、すでにハードコピーとして出力されている文書の管理には適用できない。

【0007】 本発明は、上記問題点に鑑み、書類やその複写の機密管理のための、より実用的な手段を提供することを目的とする。より具体的に述べれば、本発明の一つの目的は、書類あるいはその複写に、当該書類を最初に入手した、あるいは複写した者あるいは部署等の氏名や名称、その他、当該文書の機密管理に役立つ情報を、

50

容易に改竄することができず、かつ確実に再現できる形で付加する手段を提供することにある。本発明のもう一つの目的は、書類やその複写より、その機密管理に役立つ情報を自動的に再現する手段を提供することにある。

【0008】

【課題を解決するための手段】上記目的を達成するための本発明の骨子は、機密管理用画像のフーリエ変換データを点の集合の形にエンコードして書類の画像に埋め込んでおくことと、書類またはその複写の画像より、フーリエ変換データを復元して逆フーリエ変換を行なうことにより、書類の画像に埋め込まれている機密管理用画像を再現することである。

【0009】

【作用】本発明によれば、書類の内容を読み難くすることなく、機密管理用画像の情報を書類の画像に埋め込むことができる。また、書類を見ただけでは埋め込まれた機密管理用画像の内容を理解できないことは勿論のこと、当事者以外の者には、機密管理用画像が埋め込まれていること、あるいは当該書類が機密扱いであることを気付かれない。

【0010】また、本発明によれば、機密管理用画像はフーリエ変換後に点の集合の形にエンコードされて書類の画像に埋め込まれるので、そのエンコードデータの一部が欠落しても機密管理用画像を再現することができるため、書類の画像に埋め込まれた機密管理用画像の情報の改竄はほとんど不可能であり、また、書類の複写を繰り返すことにより画像品質が劣化しても、そこに組み込まれた機密管理用画像を再現可能である。しかも、機密管理用画像の再現の自動化、さらには、その内容の自動認識も容易である。

【0011】したがって、本発明によれば、機密扱いの書類やその複写が第三者の手に渡ったような場合に、当該書類を最初に配布された者、複写をとった者、部数、日時等の情報を当該書類または複写より確実に取得して当該書類や複写の流出経路を調査する等、機密管理のための措置を容易確実に講じることが可能である。

【0012】

【実施例】以下、本発明の実施例について図面を用いて説明する。本発明によれば、書類を新規に作成する際、あるいは既に作成された書類を複写する際に、当該書類の流出経路追跡等の機密管理に役立つ情報、例えば作成もしくは複写した日時、作成もしくは複写した人の氏名、作成もしくは複写した部数等を、画像情報の形で書類そのものの画像に埋め込む。そして、不当に流出した書類または複写を見発した場合には、そこに埋め込まれた画像情報を再現することによって、その流出経路等の追跡に利用する。

【0013】まず、流出経路の追跡等に役立つ機密管理用画像情報を埋め込むプロセスの一例について説明し、次に書類または複写より、そこに埋め込まれた機密管理

用画像情報を再現するプロセスの一例について説明する。

【0014】<画像情報の埋め込みプロセス>このプロセスを図1乃至図5によって説明する。図1はプロセスの概略フローチャートであり、図2は同プロセス中でのデータの変遷の様子を模式的に示している。

【0015】最初のステップ101において、書類（またはその複写）の画像に埋め込みたい機密管理用画像のデータの高速フーリエ変換（FFT）を実行し、W（幅）×H（高さ）の大きさの機密管理用画像（110）に対して、実部及び虚部ともにW（幅）×H（高さ）の大きさのフーリエ変換データ（112）を得る。

【0016】つぎのステップ102において、前ステップで得られたフーリエ変換データ（112）の実部及び虚部をそれぞれ別々に、2値の画素の集合で表わされたエンコードデータ（113）に変換する。

【0017】このステップ102の内容をより具体的に述べれば、例えば、フーリエ変換データの実部と虚部それを、0から15までの16値に量子化する。そして、量子化後の各点の値を図3に示すような重み付けをした2×2の2値画素パターンによって表現する。各点の値と4画素パターンとを対応させて図4に示す。なお、図4の各パターンにおいて、網掛けされた格子は黒画素であることを意味し、白地の格子は白画素であることを意味している。

【0018】このようにして実部と虚部の各点を表わす2×2画素パターンを、各点の配列に対応させて例えば図5に示すように並べることにより、フーリエ変換データを2値画像化する。なお、この例は虚部のパターンを上側、実部のパターンを下側とした2段配列であるが、一定の規則性のある他の配列方法に変更することもできる。例えば、実部と虚部のパターンを交互に上下に並べた配列とすることもできる。

【0019】図1の最後のステップ103において、前のステップで得られたエンコードデータ（113）と書類（または複写）の画像（114）との合成を行ない、それらの合成画像（115）を得る。この合成は例えば単純なOR演算により行なってよい。

【0020】この合成画像をプリントアウトした書類は、機密管理用画像のエンコードデータが重ね合わせられているが、元の書類の可読性には全く問題がない。また、関係者以外は、処理後の画像を見ただけでは、それが機密文書であることにも、機密管理のための画像情報が埋め込まれていることにも気付くことはなく、ましてや埋め込まれた画像の内容は全く理解できない。

【0021】<埋め込まれた画像情報の再現プロセス>このプロセスを図6及び図7によって説明する。図6はプロセスの概略フローチャートであり、図7は同プロセス中でのデータの変遷の様子を模式的に示している。

【0022】ステップ201において、書類（または複

写)の画像(210)より、大きい黒画素連結成分を除去する。具体的には、黒画素連結成分を抽出し、その画素数が一定値を超えるものの全ての画素を白画素に置き換えるという操作を行なう。この目的は、前述の「画像埋め込みプロセス」で合成されたエンコードデータだけを抽出することである。ただし、合成されたエンコードデータ中の文字等と重なった部分のデータは失われる。

【0023】ステップ202において、前ステップで大きな黒画素連結成分を除去された画像データ(211)より、フーリエ変換データを抽出する。このデコード処理は具体的には、図5で説明したように、一定の規則に従ってフーリエ変換データの虚部と実部の各点の値が 2×2 の画素パターンで表現されているので、それぞれのパターンを元の0から15までの値に戻す処理である(図4参照)。

【0024】ステップ203において、前ステップにより得られたフーリエ変換データ(211)の逆高速フーリエ変換(逆FFT)を行ない、埋め込まれた画像のグレイレベル画像(213)を得る。この画像をそのまま再現しても、その内容は可読である。しかし、本実施例では埋め込まれる機密管理用画像を2値画像とし、かつ画像を2値で出力することを想定しているため、本ステップ203により得られたグレイレベルの画像を次のステップ204により2値化して、埋め込まれた機密管理用画像(214)を再現する。

【0025】このようなプロセスによる機密管理用画像の再現性は良好である。画像をフーリエ変換をしてから埋め込むため、その一部のデータが欠落しても再現性が良い。書類の複写を繰り返しても、埋め込まれた画像の再現が可能であり、また、書類に埋め込んだ機密管理用画像情報を改竄しにくい。また、この埋め込み画像の再生プロセスは、前記特開平4-310175号公報の機密文書管理方式のような人手の介在を格別必要とせず、処理を自動化することが容易である。

【0026】次に、上に説明したプロセスを実施するための装置構成の例を説明する。図8は上述の「画像埋め込みプロセス」を実現するための装置構成の一例を示す概略ブロック図である。

【0027】図8において、301は一時記憶としてのメモリを内蔵したCPU(中央処理装置)、302はCPU301上で図1のステップ101の処理を実現するためのFETプログラムを格納したROM、303はCPU301上で図1のステップ102の処理を実現するためのエンコードパターン作成プログラムを格納したROM、304はCPU301上で図1のステップ103の処理を実現するための画像合成プログラムを格納したROMである。305は機密書類や埋め込み画像のデータを入力するための画像データ入力部である。この画像データ入力部305は、具体的には、フロッピーディスク等の記憶メディアやファクシミリ等の通信メディアに

よって画像データを入力する手段、あるいはワードプロセッサ等のソフトウェア手段等々である。306は、紙上に記録された書類または複写の画像あるいは埋め込まれる機密管理用画像等の画像を光学的に読み取って入力する画像光学入力部(スキャナ)である。したがって、ここに示す装置によれば、書類を新規に作成する場合に管理のための画像を埋め込むこともできるし、すでに作成された書類あるいはその複写に対して、管理のための画像を埋め込むこともできる。307は、各入力部305、306より入力された画像データや処理過程で生成された画像データを保存するために利用されるRAMである。308は画像を紙上に2値出力するための画像出力部である。なお、オペレータ操作のためのキー入力部等も存在するが図中省略されている。

【0028】機密管理用画像の埋め込まれた書類を新規に作成したい場合、対象の書類の画像と機密管理用画像を画像入力部305から入力する。ただし、書類がハードコピーとして存在するときには、その画像を画像光学入力部306より入力する。機密管理用画像も同様に、20画像光学入力部306より入力してもよい。入力された画像データは画像保存用RAM307に蓄積され、それに対してCPU301によって画像埋め込みプロセスが実行される。すなわち、FFTプログラム(302)に従って図1のステップ101の処理が実行され、その結果に対してエンコードデータ作成パターンプログラム(303)により図1のステップ102の処理が実行される。これによって得られたエンコードデータと書類画像との合成処理(図1のステップ103)が画像合成プログラム304に従って実行され、その結果が画像出力部302により紙に出力される。

【0029】なお、機密管理用画像と書類画像との合成画像のデータをフロッピーディスク等の記憶メディアに記録しておき、必要な場合に、同記憶メディアに記憶された合成画像データを本装置あるいは他の装置によってプリントアウトさせるようにしてもよい。あるいは、合成画像データをファクシミリ等で伝送し、離れた場所でプリントアウトさせることができるようにしてよい。

【0030】以上述べたことから理解されるように、この装置は、機密扱いの書類を新規に作成する場合に利用できるとともに、既に紙に出力された書類の複写を作成する場合にも、つまり複写機としても利用でき、そのいずれの場合に必要な機密管理用画像情報を書類に付加することができる。

【0031】図9は上述の「埋め込み画像再現プロセス」を実現するための装置構成の一例を示す概略ブロック図である。図9において、401は一時記憶としてのメモリを内蔵したCPU(中央処理装置)、402はCPU401上で図6のステップ201の処理を実現するための連結成分抽出プログラムを格納したROM、403はCPU401上で図6のステップ202の処理を実

現するためのデコードプログラムを格納したROM、404はCPU401上で図6のステップ203の処理を実現するための逆FFTプログラムを格納したROMである。405は、CPU401上で図6のステップ204の処理を実現するための2値化プログラムを格納したROMである。406は、紙上に記録された書類あるいはその複写の画像を光学的に読み取って入力する画像光学入力部(スキャナ)である。407は、画像光学入力部406より入力された画像データや処理過程で生成された画像データを保存するために利用されるRAMである。408は埋め込み画像の再現画像等の画像を紙上あるいはディスプレイ画面上に出力するための画像出力部である。

【0032】409はCPU401上で画像判定処理を実現するための画像判定プログラムを格納したROMである。この画像判定処理は、画像光学入力部406より入力された書類の画像より再現された埋め込み画像と、予め登録された機密管理用画像とを比較し、再現された埋め込み画像が登録された機密管理用画像と一致するか判定する処理である。この判定は、画像を直接扱う方法でも、画像中の文字あるいは記号を認識し、認識結果として得られたコードにより一致を調べる方でもよい。いずれにしても、判定で一致がとれた場合には、入力書類が機密管理用画像情報の埋め込まれた機密扱いの書類であるということである。なお、オペレータ操作のためのキー入力部等も存在するが図中省略されている。

【0033】ハードコピーとして存在する書類に埋め込まれた機密管理用画像情報を再現したい場合、その書類の画像を画像光学入力部406より入力する。入力された画像データは画像保存用RAM407に蓄積され、それに対してCPU401によって埋め込み画像再現プロセスが実行される。すなわち、連結成分抽出プログラム(402)に従って図6のステップ201の処理が実行され、その結果に対してデコードプログラム(403)により図6のステップ202の処理が実行される。これによって得られたデータに対して逆FFTプログラム(404)に従って図6のステップ203の処理が実行され、その結果に対して2値化プログラム(405)に従って図6のステップ204の処理が実行されることにより、埋め込み画像データが得られる。この再生された埋め込み画像データに対し、画像判定プログラム(409)に従って画像判定が行なわれ、その判定結果、あるいは判定結果と埋め込み画像とが画像出力部408より出力される。なお、埋め込み画像を登録する場合、その画像を画像光学入力部406より画像情報として入力することも、図示されていないキー入力部よりコードデータとして入力することもできる。

【0034】このように、この装置によれば、書類またはその複写より、そこに埋め込まれた機密管理用情報の再現とその判定を行なうことができる。

【0035】図10は、上述の画像情報の埋め込みプロセスと画像情報の再現プロセスの両方が可能な装置の構成の一例を示す概略ブロック図である。この装置は、図8に示した装置に図9に示した装置の必要な機能部を追加したごとき構成であるので、同一部分に同一符号を付すことによって説明にかえる。

【0036】つぎに、画像の埋め込みプロセスと再現プロセスの他の例を、図11及び図12により説明する。

【0037】図11は画像埋め込みプロセスの概略フローチャートである。ステップ501、502は図1のステップ101、102と同一の処理ステップである。そして、ステップ503において、機密管理用の埋め込み画像情報のフーリエ変換データのエンコードデータを、書類画像データとは別の色で、重ねてプリントアウトする。したがって、この例ではカラー出力が前提である。

【0038】図12は埋め込み画像再現プロセスの概略フローチャートである。ステップ601は書類またはその複写(ただしカラー複写)より読み取った画像データより、画像埋め込みプロセスにおいてエンコードデータの出力に用いられた色の成分だけを抽出する。ステップ602、603、604は図6のステップ202、203、204と同一の処理ステップである。

【0039】このように、フーリエ変換データのエンコードデータの出力色を書類そのものの記録色と異ならせる方法は、大きな黒画素連結成分を除去する方法によるエンコードデータの抽出が難しいようなケースに、その抽出が容易になる等の利点がある。

【0040】上に述べたプロセスを実現するための装置構成は、図8乃至図10に示したものと同様でよい。ただし、画像出力部308はカラー出力が可能でなければならず、画像光学入力部306、406はカラー画像読み取りが可能でなければならぬ。また、ROM304も図11のステップ503の処理内容に合わせたプログラムを格納したものに変更し、ROM402も図12のステップ601の処理内容に合わせたプログラムを格納したものに変更する。

【0041】

【発明の効果】本発明によれば、(1)書類を読み難くすることなく、機密管理用情報を書類あるいはその複写に付加することができる。(2)書類または複写に付加した機密管理用情報の改竄を、ほぼ完全に防止できる。

(3)書類の複写を繰り返しても、機密管理用情報を再現可能である。(4)機密管理情報の内容あるいは書類が機密扱いであることを第三者に秘諾できる。(5)書類または複写に付加された機密管理用情報の再現やその認識の処理の自動化が容易である。(6)機密管理用情報を利用した書類やその複写の流出経路の追跡等の機密管理を確実に行なうことができる等の効果を得られる。

【図面の簡単な説明】

50 【図1】画像情報埋め込みプロセスの一例を示す概略フ

ローチャートである。

【図2】画像情報埋め込みプロセス中の画像データの変遷の様子を示す図である。

【図3】フーリエ変換データの表現のための画素マトリックスを示す図である。

【図4】フーリエ変換データの値と画素パターンとの対応図である。

【図5】フーリエ変換データの実部と虚部の画素パターンの並べ方の一例を示す図である。

【図6】埋め込み画像再現プロセスの一例を示す概略フローチャートである。

【図7】埋め込み画像再現プロセス中の画像データの変遷の様子を示す図である。

【図8】画像埋め込みプロセスを実現するための装置構成の一例を示す概略プロック図である。

【図9】埋め込み画像再現プロセスを実現するための装置構成の一例を示す概略プロック図である。

【図10】画像埋め込みプロセス及び埋め込み画像再現プロセスを実現するための装置構成の一例を示す概略ブ

ロック図である。

【図11】画像埋め込みプロセスの他の例を示す概略フローチャートである。

【図12】埋め込み画像再現プロセスの他の例を示す概略フローチャートである。

【符号の説明】

301, 401 CPU

302 FFTプログラム格納ROM

303 エンコードパターン作成プログラムROM

304 画像合成プログラムROM

305 画像入力部

306, 406 画像光学入力部

307, 407 画像保存用RAM

308, 408 画像出力部

402 連結成分抽出プログラムROM

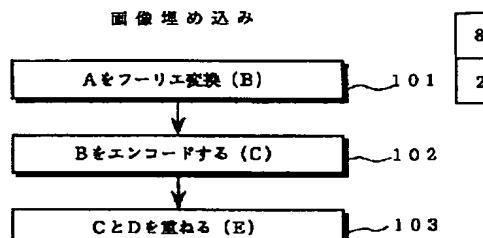
403 デコードプログラムROM

404 逆FFTプログラム

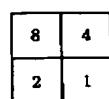
405 2値化プログラムROM

409 画像判定プログラムROM

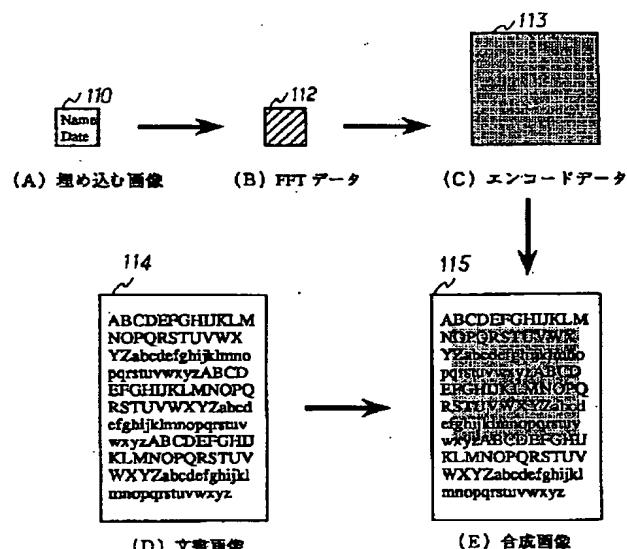
【図1】



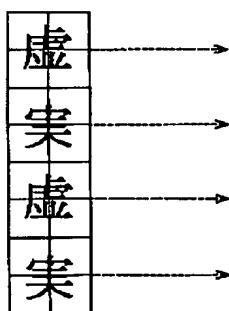
【図3】



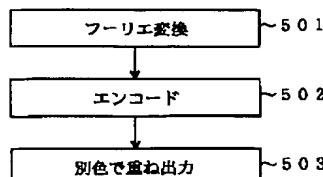
【図2】



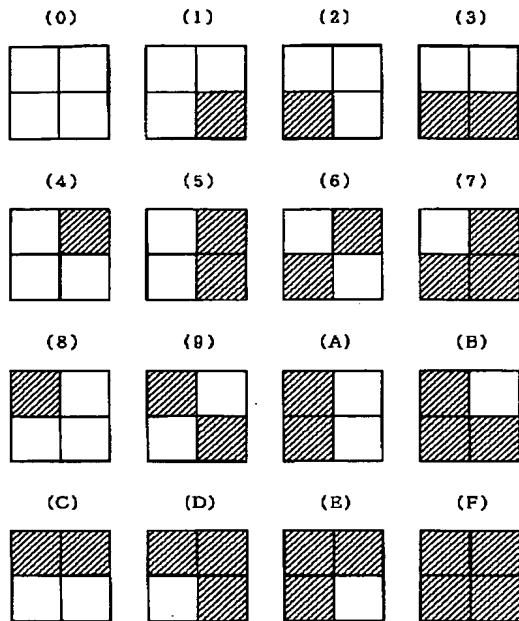
【図5】



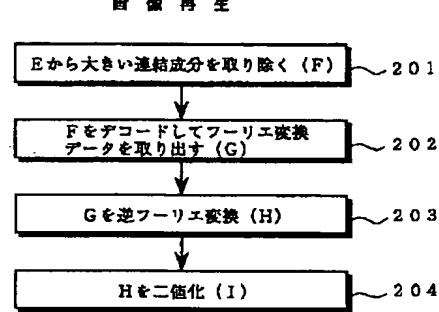
【図11】



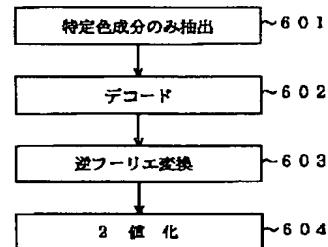
【图4】



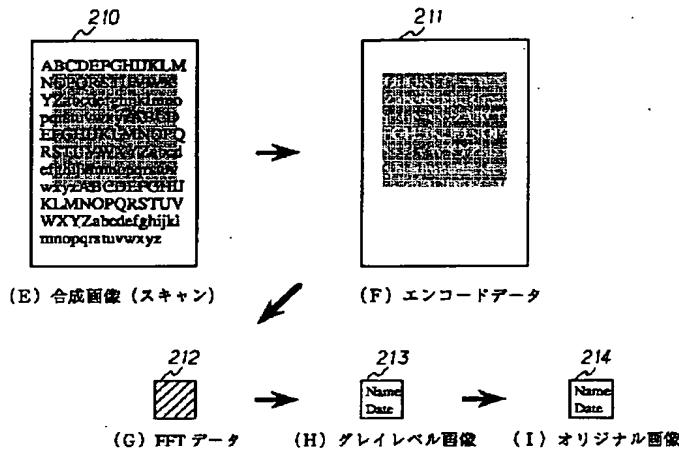
【四六】



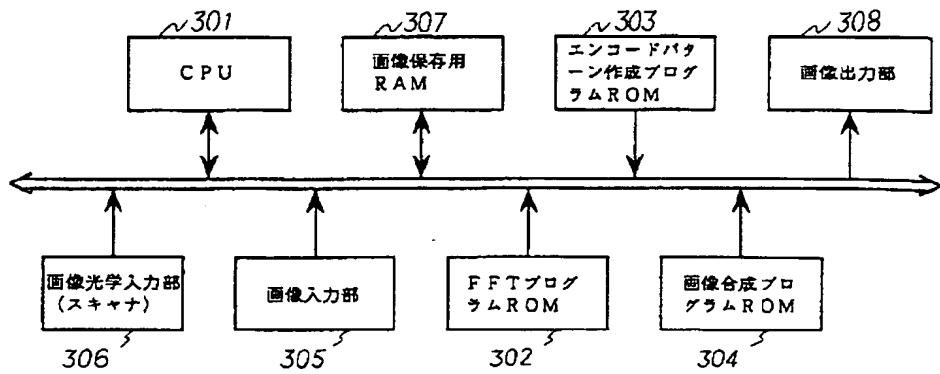
【図12】



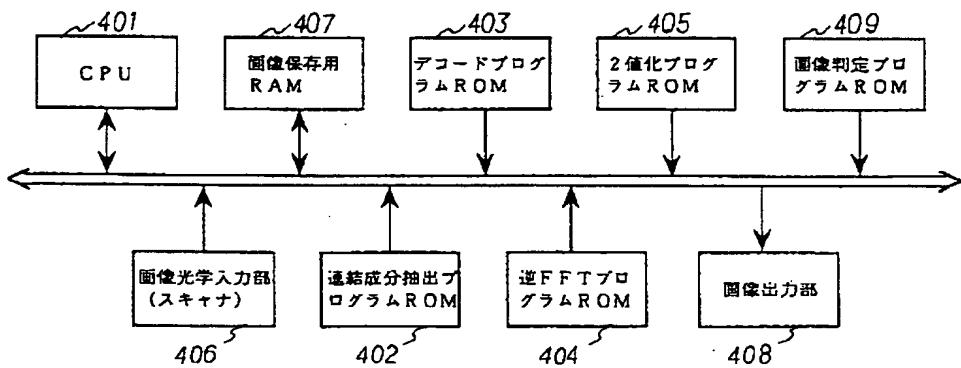
【図7】



【図8】



【図9】



【図10】

